PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 11/30 — A1

(11) International Publication Number: WO 00/48076

(43) International Publication Date: 17 August 2000 (17.08.00)

(21) International Application Number: PCT/US00/03692

(22) International Filing Date: 11 February 2000 (11.02.00)

(30) Priority Data:
09/249,043 12 February 1999 (12.02.99) US

(71) Applicant: ARCOT SYSTEMS, INC. [US/US]; 811 Hansen Way, Palo Alto, CA 94304 (US).

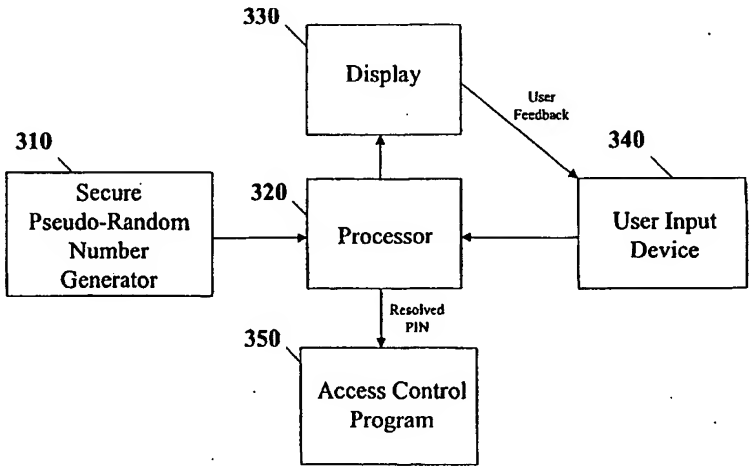
(72) Inventor: HOOVER, Douglas; 647 Sierra Vista Avenue, Mountain View, CA 94043 (US).

(74) Agents: LAURIE, Ronald, S. et al.; Skadden, Arps, Slate, Meagher & Flom LLP, Suite 220, 525 University Avenue, Palo Alto, CA 94301 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: METHOD AND APPARATUS FOR SECURE ENTRY OF ACCESS CODES IN A COMPUTER ENVIRONMENT



(57) Abstract

A user inputting his access code into a computing environment to access a transaction is at risk of losing the access code to an attacker who has physical or electronic access to the computing environment. To minimize this risk, the access code can be entered via a plurality of user–selectable fields, each of which takes on a series of values in the initial display (330). The initially displayed values are established in a random or otherwise unpredictable manner using a pseudo–random number generator (310). The user then uses a mouse, keyboard, or other input device (340) to increment each of the selectable fields until the access code is correctly entered. Because of the randomization of the initial state, an attacker tracking the locations or number of mouse clicks or other navigation actions can not determine the finally entered access code by, e.g., computing the offset from a known inital state.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

METHOD AND APPARATUS FOR SECURE ENTRY OF ACCESS CODES IN A COMPUTER ENVIRONMENT

Background of the Invention

In a computer environment, access to a transaction (e.g., obtaining secret data kept on a computer, ordering a good or service via the computer, or accessing funds at an automatic teller machine (ATM) or point of sale (POS)) is usually protected by a personal identification number (PIN), a password, or other access code. When the user wishes to conduct the transaction, he types in his access code, and is allowed access (e.g., via an access control module) if the entered value correctly matches a stored value. A typical piece of data that is protected in such way is a user's private key, which can constitute a user's identity over the Internet or some other system that uses public key cryptography for user identification. If the attacker can get access to this private key, he can impersonate the user, read information intended to be private to the user, and conduct still other electronic transactions in the user's name.

An attacker might physically gain access to the user's computer physically, or do so electronically by loading a virus onto the user's computer. In either case, the attacker can then install a program that collects, and saves to a file, all the keystrokes that the user types on his keyboard. This file can be retrieved later, either via physical access to the machine or over a network, allowing the attacker to deduce the access code by examining the user's keystrokes. Besides keyboard entry, the access code could also be inputted by selecting, via a mouse, digits or letters (more generally, characters) from a predetermined pattern of user-selectable fields (e.g., a visual representation of a telephone, typewriter, or calculator keypad) displayed on a graphical user interface (GUI). In this scenario, the attacker could obtain information about the access code by capturing the locations (e.g., x- and y- coordinates) of mouse clicks and using them to deduce the characters indicated -- since the locations of all possible characters on the interface occur in a known and fixed pattern (e.g., on a telephone-style keypad: Row 1 = 1, 2, 3; Row 2 = 4, 5, 6; Row 3 = 7, 8, 9; and Row 4 = *, 0, #).

Even where the locations of all the alphanumeric characters are not known, an attacker could still deduce the access code when an initial state of the character fields is known. For example, consider simulating and displaying an in-line combination lock having

an initial state of 0-0-0. The user then uses mouse clicks to turn the wheels (tumblers, rings, etc.) of the lock to input his access code. When the digits of the proper combination are all aligned in their proper positions, the lock "opens" (i.e., grants the user access to the desired transaction). An attacker knowing the initial state and the history of the mouse clicks could determine the access code by using the history as an offset from the initial state.

All of the foregoing shows that there is a need for protecting a user's PIN, password, or other access code, from disclosure to an attacker who, directly or indirectly, obtains the sequence of characters inputted by a user to gain access to a transaction.

Detailed Description of the Invention

To prevent an attacker from using histories of the keyboard arrowing, mouse clicking, or other navigation or selection techniques to determine the access code, the present invention randomizes (or pseudo-randomizes or otherwise makes unpredictable) the initial state of the displayed user-selectable fields. Techniques for implementing randomizing logic or modules are well known to those skilled in the art and need not be described in detail here. As an example of displaying user selectable fields, if the display visually imitates a keypad, its numbers can be randomly scrambled after each access code entry (e.g., Row 1 = 4, 6, #; Row 2 = 2, 9, 8; Row 3 = *, 1, 3; Row 4 = 0, 5, 7). Thus, an attacker who is unable to deduce the initial states of the user-selectable fields can not deduce the access code even if the attacker knows the history of the subsequent mouse clicks or other screen navigation actions. Effectively, the user's input appears to the attacker to be a random series of selections.

Alternatively, if the display depicts a combination lock, it is not necessary to scramble the characters (e.g., numbers) on the wheels, but only to start each wheel in an unpredictable position. That is, the numbers around the periphery of each wheel can still be ordered sequentially, as long as the wheels are initialized randomly. The wheels have the further advantage of being able to accommodate an arbitrarily large character set (e.g. all 26 letters of the alphabet and all 10 digits, if desired), whereas a scrambled keypad containing a large number of letters and digits might be inconvenient to use because of the difficulty in locating any desired letter or digit.

In yet another embodiment, shown in Figure 1, a randomly initialized "bingo card" could be displayed, with the user entering the PIN by clicking on the correct character in each

column of the bingo card. The current PIN could be displayable adjacent to the bingo card (Figure 1) or the selected PIN characters could be highlighted on the bingo card, e.g. by changing the color or shading of the selected characters.

In still other embodiments, the user-selectable fields could be simply displayed as a series of character boxes, much like a crossword puzzle or fill-in-the blank game, with each field being initialized to an unpredictable alphanumeric character. For example, for a six-digit PIN, the system starts by displaying six random digits. To select his PIN, the user cursors through the digits. At each digit, he hits the up or down arrow key (to increment the digit by +1 or -1) an appropriate number of times until the desired digit appears.

Alternatively, as shown in Figure 2, each particular, initially random PIN digit could be adjusted to the correct value by clicking on the corresponding "+" or "-" buttons.

Alternatively, two rows of digits could be used. One row could display an initially random PIN digit sequence. The user would input to an adjacent row an offset digit sequence such that the correct PIN digit sequence was formed when the offset digit sequence row was added to the initially random PIN digit sequence row. The resulting correct PIN digit sequence could be displayed adjacent to the other two rows.

In any of the above embodiments, an attacker might be able to examine what is displayed on the screen as the user inputs the access code, either through software or by physically looking over the user's shoulder. To defeat this attack, a particular user-selectable field could be made effectively unreadable by darkening it so that its value is not visible except when the mouse or cursor is over that field. Similarly, one or more fields could be made unreadable by replacing fields, other than the one being instantaneously inputted, with asterisks (e.g., see Fig. 1 or Fig. 2) or other non-informational characters, before or after they are selected or entered on the screen. In these ways, the attacker's opportunities to read the characters of the access code as they are entered on the screen are minimized.

Figure 3 shows a schematic of an exemplary apparatus for secure entry of an access code for secure access to an electronic service, including a hardware or software based secure psuedo-random number generator 310 providing an initially randomized input to processor 320 for display to a user on display 330. Based on the display, the user provides feedback (in the form of an entered access code) via input device 340, which is passed back through processor 320 to access control program 350. Note that a non-visual "display" 330 is also possible, e.g. feedback via audio headphones or other output devices. The feedback to the

user, whether by visual display or other means, should be harder for an attacker to intercept than the user input.

A wide variety of techniques (e.g. software or hard-wired instructions running on processor 320) can be used for implementing the foregoing user-selectable fields in various environments (e.g. accepting them via input device 340 and displaying them via display 330) including, without limitation, the following:

(a) In an Internet environment, the user-selectable fields could be implemented (i) using Javascript on a web page to send the PIN to a common gateway interface (CGI) script or active server page, (ii) using a Java applet on a web page to send the PIN to a CGI script or active server page, (iii) using a plug-in with a GUI on a web page to send the PIN to a CGI script or active server page, (iv) using a specialized network application with a GUI to send results by a network connection to a server application, or (v) using a specialized network application with command line input.

(b) In a stand-alone computing environment, the user-selectable fields could be implemented (i) by GUI, (ii) by command line entry using the offsets to an initial value method, or (iii) by use of a machine logon method.

(c) In a network PC environment or a personal digital assistant environment, the user-selectable fields could be implemented using the methods just described for an internet environment or a stand-alone computing environment.

(d) In an ATM or POS environment, the user-selectable fields could be implemented directly on processor 320 via an application specific integrated circuit (ASIC), programmable logic array (PLA), or microcode and displayed on a touch screen or keypad.

These and many other techniques for implementing and displaying the user-selectable fields are well known to those skilled in the art, and need not be described in greater detail here.

Similarly, a wide variety of input devices 340 could be used for inputting the user-selectable fields including, without limitation, a keyboard, a mouse, a touch pad, a think screen, or other pointing devices. Hardware and program logic code for implementing and controlling these devices are well known to those skilled in the art and need not be described in detail here. Finally, although the various embodiments have disclosed alphanumeric characters, the

displayed fields are not strictly limited to alphanumeric characters, but could also include mathematical symbols or discrete elements of ideographic languages such as Japanese or Chinese. It should therefore be understood that references to "alphanumeric" or "character" include all these and still other linguistic or symbolic elements with which an access code can be represented.

Those skilled in the art will readily appreciate that all the foregoing (and many other) techniques known to those skilled in the art for creating and displaying visual fields, for inputting the access code, and for the format of the access code, can be used in conjunction with the present invention. It is therefore intended that the scope of the invention be not limited to the particular embodiments disclosed herein, but rather to the full breadth of the claims appended hereto.

CLAIMS

What is claimed is:

1. A method for secure entry of an access code for secure access to an electronic service, comprising the steps of:
   (a) randomizing a plurality of fields selectable by a user to input an access code;
   (b) displaying, via a graphical user interface, a plurality of selectable fields;
   (c) accepting, from said user, a plurality of selections chosen from among said fields;
   (d) granting, to said user, access to a service if said accepted plurality of selections correctly correspond to a predetermined access code.

2. The method of claim 1 where said selectable fields include a plurality of alphanumeric characters.

3. The method of claim 1 where said user selections are accepted from said user via a pointing device.

4. The method of claim 3 where said pointing device is a touch screen.

5. The method of claim 3 where said pointing device is a mouse.

6. The method of claim 1 where said user selections are accepted from said user via a keyboard.

7. The method of claim 1 where said user selections are accepted from said user via an incrementing arrow in said graphical user interface.

8. The method of claim 1 where said step of displaying said selectable fields include displaying a visual form of a keypad containing said fields for viewing by said user.

9. The method of claim 1 where said step of displaying said selectable fields includes displaying a visual form of a plurality of rotatable wheels for viewing by said user.

10. The method of claim 1 where said step of displaying said selectable fields includes displaying a representation of a bingo card for viewing by said user.

11. The method of claim 1 where said step of displaying said selectable fields includes displaying at least one of said fields as unreadable except when said one of said fields is being selected by said user.

12. The method of claim 11 where said step of displaying said field as unreadable includes displaying a darkened field.

13. The method of claim 11 where said step of displaying said field as unreadable includes displaying a non-informing character.

14. The method of claim 1 where said step of randomizing said selectable fields is performed after accepting a previously inputted user selection of said fields.

15. An apparatus for secure entry of an access code for secure access to an electronic service, comprising:

(a) a randomizing module for initializing a plurality of fields selectable by a user to input an access code;

(b) an output device configured to display, to said user, said plurality of selectable fields;

(c) an input device configured to accept, from said user, a plurality of selections chosen from among said fields; and

(d) an access control module configured to grant, to said user, access to an electronic service if said plurality of selections correctly corresponds to said access code.

16. The apparatus of claim 15 wherein said service includes an automatic teller machine transaction.

17. The apparatus of claim 15 wherein said output device is configured as a graphical user interface.

18. The apparatus of claim 17 wherein said graphical user interface is an Internet browser.

19. The apparatus of claim 15 wherein said output device is an audio device.

20. A computer-readable medium containing logic instructions for secure entry of an access code for access to an electronic service, said logic instructions comprising:

(a) randomizing program code configured to initialize a plurality of fields selectable by a user to input an access code;

(b) display program code configured to present, to said user, said plurality of selectable fields;

(c) input program code configured to accept, from said user, a plurality of selections chosen from among said fields; and

(d) access control program code configured to grant, to said user, access to a transaction protected by said code if said accepted plurality of selections correctly correspond to said access code.

FIGURE 1

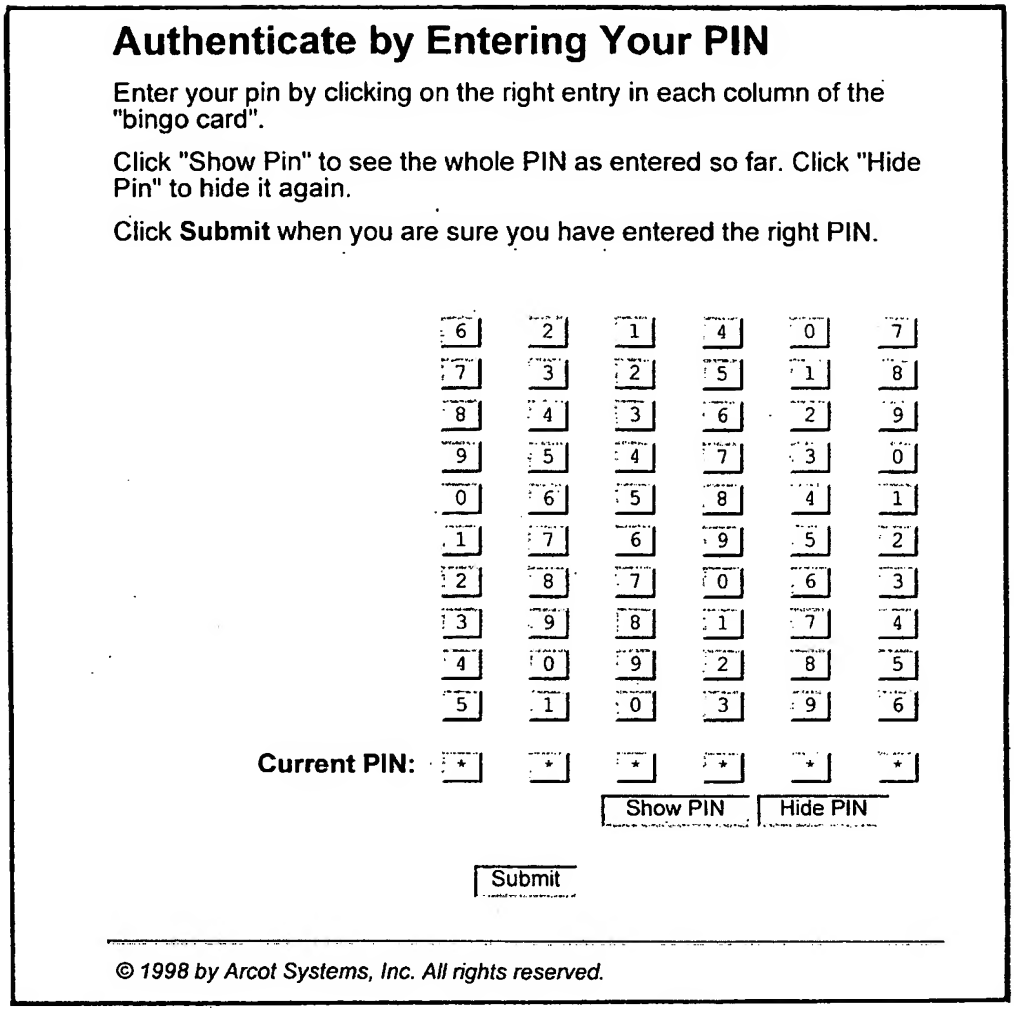

Authenticate by Entering Your PIN
Enter your pin by clicking on the right entry in each column of the "bingo card".
Click "Show Pin" to see the whole PIN as entered so far. Click "Hide Pin" to hide it again.
Click Submit when you are sure you have entered the right PIN.
6 2 1 4 0 7
7 3 2 5 1 8
8 4 3 6 2 9
9 5 4 7 3 0
0 6 5 8 4 1
1 7 6 9 5 2
2 8 7 0 6 3
3 9 8 1 7 4
4 0 9 2 8 5
5 1 0 3 9 6
Current PIN: * * * * * *
Show PIN
Hide PIN
Submit
© 1998 by Arcot Systems, Inc. All rights reserved.

FIGURE 2

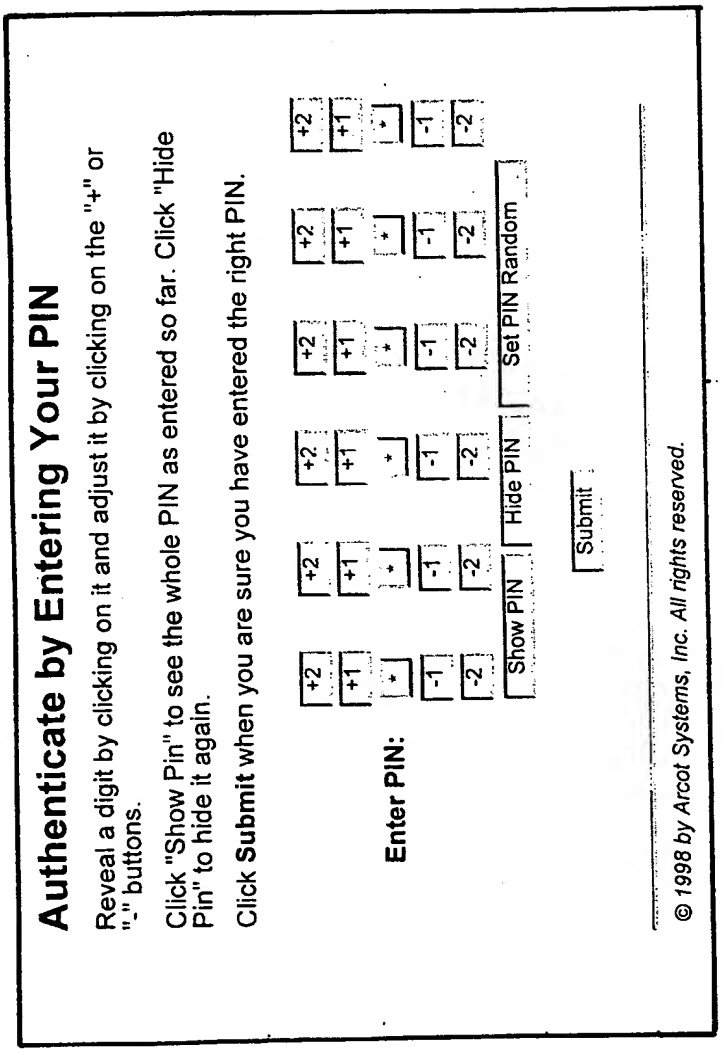
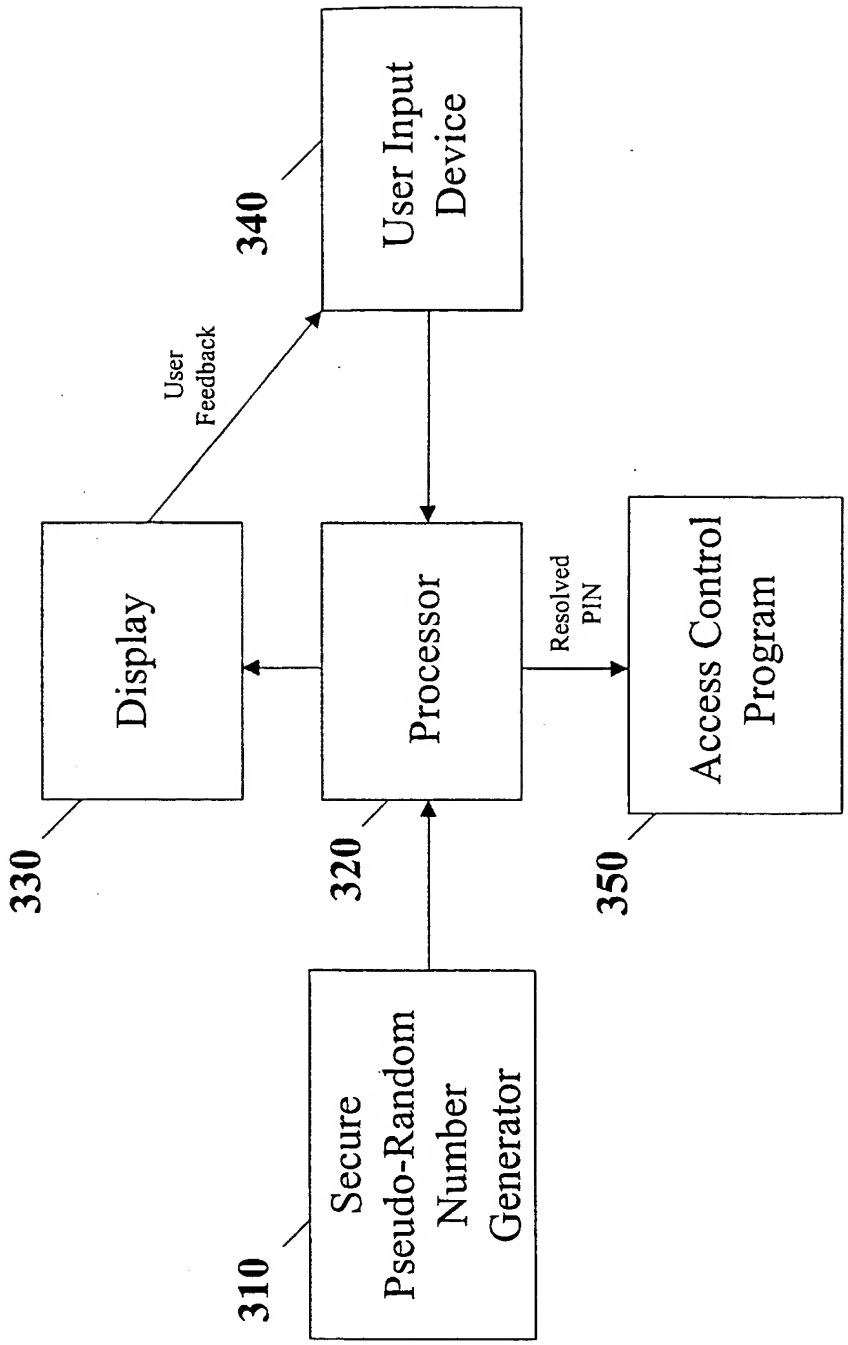

Authenticate by Entering Your PIN
Reveal a digit by clicking on it and adjust it by clicking on the "+" or "-" buttons.
Click "Show Pin" to see the whole PIN as entered so far. Click "Hide Pin" to hide it again.
Click Submit when you are sure you have entered the right PIN.
Enter PIN:
+2 +1 * -1 -2
Show PIN
Hide PIN
Set PIN Random
Submit
© 1998 by Arcot Systems, Inc. All rights reserved.

FIGURE 3


User Input Device
340
User Feedback
Display
330
Processor
320
Resolved PIN
Access Control Program
350
Secure Pseudo-Random Number Generator
310

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/03692

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 11/30
US CL : 713/200

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/200, 201, 202; 380/24

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,276,314 A (MARTINO et al) 04 January 1994, ALL	1-6,10-20
X,P	US 5,919,091 A (BELL et al) 06 July 1999, ALL	1,7-91
A,P	US 6,016,504 A (ARNOLD et al) 18 January 2000, Figure 5	13

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
27 APRIL 2000	23 MAY 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Thomas Lee Telephone No. (703) 308-7090

Form PCT/ISA/210 (second sheet) (July 1998) ★

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/03692

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

WEST, EAST
search terms: security, access control, ATM, atuomatic teller machine, network, internet, firewall, passwork, pin, id, graphical display, interface, audio, random, adjustable, etc.

THIS PAGE BLANK (USPTO)